BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer merupakan teknologi yang perkembangan sangat pesat saat ini. Hampir disetiap perusahaan, istansi pemerintahan, sekolah, rumah sakit, perguruan tinggi, masjid dan disetiap tempat pada saat ini umumnya terdapat jaringan komputer. Internet pada saat ini adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraksi. Tetapi dengan banyak komputer yang terhubung bisa menjadi ancaman berbahaya yang dapat menimbulkan terjadi serangan, baik dari dalam maupun luar seperti virus, trojan maupun *hacker*.

Ancaman serangan pada jaringan merupakan masalah yang sangat banyak dan semakin pesat perkembangannya saat ini. Seperti kasus yang diberitakan dari Tempo (2017) serangan jaringan komputer yang telah merugikan Bank Sentral Negara Bangladesh pada Februari 2016. Bank tersebut diretas oleh *hacker* yang dinilai memiliki hubungan dengan Korea Utara, mendapatkan $81 juta (sekitar Rp 1,08 triliun). Kompromi terhadap akun-akun Swift, digunakan untuk memindahkan uang antarnegara adalah alasan utama mengapa komputer-komputer dalam bank sentral Bangladesh bisa diretas.

Serangan-serangan pada jaringan komputer semakin berkembang dan jaringan komputer rentan dibobol sehingga merugikan pengguna jaringan. Salah satu contoh bentuk serangan seperti *Buffer Overflow, DOS attack, SMB Probes, OS Fingerprint* dan lain-lain (Takyudin, 2012). Serangan dapat membuat tiga aspek penting dalam jaringan komputer menjadi terganggu yaitu: penyusup mempunyai akses ke informasi atau data rahasia, keaslian informasi dapat dimodifikasi oleh penyerang dan ketersedian akan informasi menjadi tidak dapat digunakan secara normal (Soleiman dan Fetanat, 2014).

KDD *(Knowledge Discovery and Data Mining) dataset Cup* 1999 merupakan salah satu contoh data serangan jaringan yang berhasil ditangkap pada jaringan

komputer. *KDD dataset Cup* merupakan *dataset* yang dikeluarkan oleh DARPA (*Defense Anvance Research Project Agency*) pada tahun 1998. Data ini digunakan sebagai versi data kompetisi di bidang Data Mining dan Ekplorasi ilmu pengetahuan diseluruh dunia yang diadakan oleh *ACM SIGKDD* (*Special Interest Group on Knowledge Discovery and Data Mining*). Fitur yang ada pada KDD *dataset* Cup 99 terdiri dari 41 fitur terdiri dari fitur kategoris dan numerik (Amudha dan Rauf, 2011). Pada data KDD dataset cup 1999 terdapat jenis serangan Probes, DOS, U2R, R2L dan bukan serangan (Khaerani Izza dan Handoko Budi Laksono, 2015).

Untuk mengetahui jenis serangan jaringan seperti Probes, DOS, U2R, R2L dan bukan serangan dapat dilakukan klasifikasi menggunakan mesin learning. Pada beberapa penelitian klasifikasi serangan jaringan computer menggunakan mesin learning dilakukan dengan pembelajaran Data Mining dan Jaringan Syaraf Tiruan.

Pada penelitian ini dilakukan klasifikasi serangan jaringan komputer dengan pembelajaran Jarinngan Syaraf Tiruan (JST). JST merupakan suatu model kecerdasan yang diilhami dari struktur otak manusia dan kemudian diimplementasikan menggunakan program komputer yang mampu menyelesaikan sejumlah proses perhitungan selama proses pembelajaran berlangsung (Anita Desiani dan Muhammad Arhami, 2005). Beberapa metode yang biasa diterapkan dalam jaringan syaraf tiruan untuk klasifikasi serangan jaringan komputer adalah *Learning Vector Quantization* (LVQ), *Error Backpropagation* (EBP), *Self Organizing Map* (SOM), *Feed Forward Neural Network* (FFNN), *Elman Neural Network* (ENN), *Generalized Regression Neural Network* (GRNN), *Probabilistic Neural Network* (PNN), *Feed Forward Neural Network* (FFNN) dan *Radial Basis Function* (RBF).

Pada penelitian ini digunakan metode RBF untuk melakukan klasifikasi pada serangan jaringan komputer. Metode *Radial Basis Function* merupakan struktur jaringan sederhana yang tidak perlu menggunakan perhitungan panjang. RBF Neural Network memiliki kemampuan untuk mempelajari sesuatu dengan cepat. Dalam pendekatan klasik metode *RBF Neural Network* memiliki *hidden layer* didapat dari

input data. Struktur jaringan *RBF Neural Network* terdiri dari tiga lapisan yaitu *input layer*, *hidden layer* dan *output layer* (Lu Ying Wei dkk, 1999).

Beberapa penelitian terkait menggunakan metode RBF pada klasifikasi serangan jaringan komputer dilakukan oleh Kashyap Suresh dkk, pada tahun 2013 pada penelitian tersebut dilakukan pebandingan antara metode RBF dengan metode EBP, menghasilkan kesimpulan bahwa metode RBF lebih baik dibandingkan dengan metode EBP. Kemudian penelitian oleh Devaraju S dan Ramakrishnan S, pada tahun 2013 menyatakan bahwa RBF mencapai tingkat akurasi sebesar 83,51%.

Pembentukan struktur jaringan pada RBF ditentukan oleh 3 buah parameter yang dapat disesuaikan yaitu titik pusat dan lebar jarak antara *hidden layer* dan bobot koneksi dari *hidden layer* ke *output layer*. Jumlah nilai center yang digunakan pada jaringan RBF yaitu sejumlah inputan sampai dua kali jumlah inputan (Mehta dkk, 2012). Jumlah nilai center yang diguanakan pada jaringan RBF adalah dilihat dari jumlah nilai eror terkecil pada proses pelatihan jaringan RBF. Penentuan nilai *center RBF* dilakukan dengan dua acara, secara acak dan menggunakan algoritma clustering.

Algortima clustering yang digunakan dalam menentukan nilai center yaitu menggunakan algoritma K-Means dan C-means. Pada penelitian ini penulis mengggunakan algoritma K-means dalam menentukan nilai center. Algoritma K-Means adalah proses pencarian center terbaik untuk jaringan syaraf tiruan yang terbentuk dan clustering data sesuai nilai center (Sutijo, Subantar, dan Suryo Guritno, 2006 dikutip oleh Ignatius Ricardo, 2012). Kemudian, algoritma K-means merupakan algoritma yang sering digunakan dalam pencarian nilai center (Weikuan Jia dkk, 2014).

Berdasarkan beberapa penelitian sebelumnya pada penelitian ini akan dilakukan penerapan algoritma RBF dengan jumlah center dinamis pada klasifikasi serangan jaringan komputer. Data serangan komputer yang digunakan bersumber dari KDD *dataset Cup* 1999. Diharapkan dalam penelitian ini, dapat mengklasifikasikan jenis serangan komputer lebih baik dan memiliki nilai akurasi tinggi.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, maka rumusan masalah penelitian ini adalah "Bagaimana penerapan algoritma RBF dengan jumlah center dinamis untuk klasifikasi serangan jaringan komputer menggunakan dataset KDD CUP 1999".

1.3 Batasan Masalah

Batasan masalah dalam penulisan tugas akhir ini adalah sebagai berikut:

a. Algoritma K-Means digunakan dalam penentuan nilai center.
b. Klasifikasi yang dihasilkan berupa Normal, Serangan DoS, Probe, R2L, dan U2R.
c. Data yang digunakan adalah dataset KDD CUP 1999.

1.4 Tujuan Penelitian

Penerapan algoritma RBF-L menggunakan jumlah center dinamis pada klasifikasi serangan jaringan serta tingkat akurasi yang diperoleh.

1.5 Sistematika Penulisan

Sistematika penulisan Tugas Akhir ini diatur sedemikian rupa sehingga segala kebutuhan yang dipergunakan di dalam penelitian dapat dipahami dengan mudah. Sistematika penulisan laporan Tugas Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan dasar-dasar penulisan tugas akhir yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian dan sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Bab ini berisi uraian mengenai teori-teori yang berhubungan dengan topik penelitian antara lain, Jaringan Syaraf Tiruan, Metode *Radial Basis Function*, Algoritma *K-Means*, Normalisasi, Tipe Serangan Jaringan komputer. KDD dataset cup 1999, *Confusion Matrix* dan Penelitian Terkait.

BAB III METODOLOGI PENELITIAN

Bab ini membahas langkah-langkah yang dilaksanakan dalam proses penelitian yaitu, perumusan masalah, studi pustaka, pengumpulan data dan informasi, serta alur penelitian.

BAB IV ANALISA DAN PERANCANGAN

Bab ini berisikan tentang tentang analisa dan perancangan aplikasi yang akan dibangun yang berisi mengenai penereapan algoritma RBF menggunakan jumlah center dinamis dalam melakukan klasifikasi serangan jaringan.

BAB V IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi dan pengujian yang dilakukan terhadap proses pelatiham dan pengujian terhadap metode yang digunakan.

BAB VI KESIMPULAN DAN SARAN

Pada bab ini akan dipaparkan mengenai kesimpulan yang terdapat pada penelitian dan saran untuk pengembangan penelitian selanjutnya.